Countering Surveillance with NoTrace.How

The Final Straw Radio – March 10, 2024

We're sharing a conversation with Aster, a European anarchist involved in the counter-surveillance and anti-repression project known as the No Trace Project which works to share information about known methods and cases of state surveillance. The project does this in order to improve and expand our collective knowledge, tools and abilities at evading state crackdowns as we organize and act. This interview was conducted via encrypted messages and Aster's portion is being read by an unrelated volunteer. You can find the transcript at our website.

If you plan to visit their site, we suggest at least running a VPN (riseup.net has a free one) and using an anonymized browser. One method is to download the tor browser (find your device/ operating system at ssd.eff.org for some tips) and visit the No-Trace Project tor address. Their website can also be found at **https://NoTrace.How**

Search for this interview title at **https://thefinalstrawradio.noblogs.org/** to find links to further resources on this topic, featured music, the audio version, and files for printing copies of this episode.

TFSR: Would you introduce yourself, a psuedonym and pronoun we can use maybe, what part of the world you're based in and maybe how you got interested in the technical side of activism?

Aster: You can call me Aster, my preferred pronoun is the singular they. I'm from Europe and I've been involved with the No Trace Project since its beginning about three years ago.

If by "technical side" you mean collecting texts and managing a website, I think I've always liked this kind of work. It's calm and ordered work. I think in another life I could have been a librarian.

If by "technical side" you mean working on the topics of surveillance and security: I think it first started some years ago, when I felt frustrated about how comrades around me approached these topics. I felt that they were spending a lot of time thinking about how to fight cops in the streets, the ones you encounter during demonstrations and riots, and not enough time thinking about how to fight the cops in the offices. And the cops in the offices are the investigators, the intelligence analysts, the ones that are often responsible for sending our comrades to jail for long sentences and disrupting our networks. So, I felt like there was a need to spend more time countering this aspect of repression, the surveillance, the investigations.

Also, I felt like many traditional leftist organizations were working on the issue of mass surveillance, of the "wrongful" surveillance of law-abiding citizens. The revelations made by Snowden in 2013 of the mass surveillance practices of the NSA of course helped to put the focus on that. But I felt like not enough people were working on the issue of targeted surveillance, on what the State does when they target specific people. A number of comrades around the world had of course developed thoughts on this, but I felt that these thoughts were scattered around the Internet and hard to find. So that's how the No Trace Project started: as a central place to gather zines and articles made by comrades on targeted surveillance, to make them more accessible.

TFSR: Thanks so much for speaking with us. Would you talk about the No Trace Project and how it developed? Did it develop out of any particular surveillance coming to light that you'd want to mention?

Aster: I don't think it developed out of any specific thing, but I was certainly influenced by surveillance happening around me. Some close friends were facing intense police surveillance and harassment and we didn't, in my opinion, deal with it appropriately, which led to a lot of disruption in our network, and people getting burned out. A distant friend was arrested after their DNA was found on an intact incendiary device. I was particularly frustrated about DNA in general because so many anarchists worldwide were getting arrested, and are still getting arrested, because of DNA traces. And a number of those arrests look like they could be prevented if people were better informed.

So, anyway, the No Trace Project started in 2021 as a website that collected resources, zines, articles, about surveillance. The website design was really bad at the time, it's a bit better now. We were collecting stuff but not writing our own content.

Later, we started to feel inspired to write our own content, and we decided to tackle the issue of *threat modeling*. Threat modeling is a formal exercise where you identify the threats you face in a specific context and what you can do about them. So for example, in the context of an action, you identify the techniques that the police could use against you, and how you can protect from those techniques. The result of the exercise, the list of threats, is your *threat model*.

In some anarchist circles, there's this recurring situation where someone asks what security measures they should take in such or such context, for example if they can take their phone to a demo, or what email provider they should use, and people answer "it depends on your threat model". But how does one determine what is their threat model? What surveillance techniques are available to the police, and in which contexts? And how can we protect against them? In 2023 we added a new section to our website, the "Threat Library", to try to answer those questions. It's a work-in-progress, we're adding content regularly, feel free to check it out.

Later in 2023 we got in touch with another project called "Ears and Eyes", a big database of hidden surveillance devices used against anarchists: bugs, hidden cameras, GPS trackers on vehicles. We agreed that it would be good to move their project to our website, so we did that.

And I think that's all for the current developments.

TFSR: What are some of the shorter and longer term goals of the project?

Aster: In terms of shorter goals I would say to keep our website updated, by adding new resources, new content to our Threat Library, new cases to Ears and Eyes. We have several original publications that should be released soon, including an original zine on physical surveillance, and an English translation of a French zine on DNA. Our Threat Library currently lists about twenty repressive operations that have targeted anarchists around the world and I'd like to add more, to reach maybe forty or fifty operations. We're also working on various translations with the help of external translators, I'm hoping to have our Threat Library translated to French in the next few months, and probably to Brazilian Portuguese at some point. Maybe German too.

In terms of longer goals, I guess we aim to become a good resource about surveillance and security for anarchists worldwide. I'm not yet sure what this will entail, we're discovering that as we go on. A sort of vision I have is to encourage the creation of small, decentralized groups working on issues related to surveillance and security and then sharing their work with the larger anarchist movement. A bit like affinity groups of action, but for technical research. Like, imagine a group in one country researching cheap ways to hack or take down police drones, or good protocols against DNA traces, or an analysis of thermal imaging used by police helicopters, and then sharing their research publicly so it can be used or expanded by other groups in other countries. Ideally, I'd like our project to encourage that.

TFSR: We've tried our hand in this project years ago to try to talk through some technological surveillance issues and ways people were talking about evading them based on a US model, like having easy access to unregistered sim cards and setting up psuedonymous phones, an attempt to normalize comfort around recognizing the methods we understood the state to employ. Technical knowledge and skills are an area that many people don't think they have a proclivity for and so becomes specialized, but I think of it more as a series of muscles that you strengthen through use as opposed to something innate and inborn. Is there an element of NoTraces.How of hoping to reach a wider audience who may be on the cusp of increasing their skillsets or is it mostly just directed at those technical research affinity groups?

Aster: Ah yes, that's a good question. I think in terms of *content*, we want to focus on sort of higher-end security practices, that are relevant to people who risk being targeted by the State, people who risk years or decades in prison. But we do want to encourage everyone to follow these security practices, or at least some of them, and we do want to make them as accessible as possible. We want to encourage everyone to have good security because, even if someone isn't doing anything too risky, maybe their friend does, or their friend's friend. Individual security reinforces collective security. And, just to be clear, this is not just about tech security, the majority of our content isn't about technology. And while some non-technology security practices require developing a specific skill set, for example detecting if you're being followed by cops, some other just require good communication skills, for example the need-to-know principle, which simply states that sensitive information should only be shared when it is necessary to do so, and to the extent necessary.

So then there's the question of how to make our project accessible to a variety of people, how to make it a good place to learn. We try to write our original content in a clear way that doesn't assume too much prior knowledge from our readers. All of our original content is available as printable zines so it can be read and shared away from computers. And, of course, we want to do translations, a lot of translations.

One thing I haven't talked about yet, that is somewhat related to this topic, is another reason I got involved with the No Trace Project: I wanted to codify knowledge that is often transmitted only informally in anarchist circles. At least in the circles where I was active, many security practices were not codified, were not shared in meetings or written down in zines. For example, it took me years to understand the dangers of DNA because it wasn't a topic that was discussed openly. Security practices were transmitted informally, sure, but that's not welcoming of newer or more isolated comrades who may not be part of the informal discussions. I'd like our project to be welcoming of those comrades too.

TFSR: Yeah, that seems like an important point, the codification as you put it, or at least the bringing of those practices to more peoples awareness. It also seems like there is an opportunity here for spreading the word of instances of movement surveillance and interference, anti-repression organizing and possibly mapping state and para-state strategies and methods so as to build more resilient resistance. Can you talk about this as well as possible repression or shifts in adversarial methodology you all might expect in response to the public exposure of these surveillance methods and tools. Like, could someone face charges for releasing information about this state spying? [please feel free to call out this logic in your response]

Aster: Indeed, I'd like our project to help spread the word about specific instances of repression. About instances of repression, many anarchist groups are focused on solidarity and prisoner support, and while I believe this focus is extremely important, I feel like sometimes the more factual, technical aspects of repression are neglected. So in relation to instances of repression, I'd like our project to focus on, like: "What happened? What happened for these comrades to end up in jail, or for this promising movement to disappear? If they are able to tell us, can we learn from their experiences?" And I guess that showing comrades that we take their experiences seriously and that we are dedicated to learn from them can also be a form of solidarity.

About, will the State adapt because we reveal their strategies? I think at a local level, they can adapt. For example if you notice cops following you in the streets, it's generally in your advantage to not show them that you noticed them, otherwise they will adapt and be more discreet. But at a global level, I don't think the State adapts well, and when they adapt I think it's more likely to be because of new technological developments, for example. At a global level, I think it's always in our advantage to reveal their strategies.

To the question of if someone could get charges for revealing the State strategies? Yes, certainly, people have been charged for that in the past. As always, whether a person will be charged with something has a lot to do with the political motivation of the State to charge them, which can be hard to predict. And of course, we can try to stay anonymous when we reveal State strategies, to make repression less likely.

TFSR: A lot of these examples of physical surveillance come from Europe, where you mentioned that you are from. I feel like this is the stuff we saw in the USA 15 years ago but doesn't feel as common these days.

I know the EU has much stricter privacy laws than the USA when it comes to what data tech companies can track. I wonder if this type of physical surveillance is more common in the EU because it's more necessary. In the US cops can just go to Meta/AT&T/etc. Also, with the rise of Amazon Ring we're putting the cameras up for them (despite that Amazon recently stated they'll require warrants for law enforcement access to camera footage). Could you talk about how these material circumstances (operating in the EU versus in Russia or the USA or UK) effect the approach one might take?

Aster: Before answering, I want to acknowledge that at the No Trace Project, our experience is mostly with Western Europe and North America. I'm from Western Europe, and some of our members are from North America. I want to learn more about other parts of the world but I don't feel confident to speak about them yet.

So, I think that the reasoning you suggest about physical surveillance being less common in the U.S. is flawed; I'll try to explain why I think that. Just to be clear on the terms, what I mean by "physical surveillance" is the direct observation of a target. This means that a surveillance team is on the ground to watch or follow someone, for example a suspect in a criminal case. A surveillance team is typically composed of at least five officers, and several vehicles. For law enforcement and intelligence agencies, physical surveillance is a resource-intensive and personnel-intensive surveillance method. Because these agencies have limited resources and personnel, this means that physical surveillance isn't their preferred method: if they can obtain the results they want without using it, they won't use it. Physical surveillance is used when two factors combine: first, the crime being investigated is a sufficient threat to the State, for example an arson; and second, the suspects being investigated need to be monitored but cannot be monitored by more accessible surveillance methods such as phone monitoring. In some cases investigators try to monitor a suspect's phone, or their social media, and so on, and when this doesn't provide the results they want, they resort to physical surveillance. In other cases, investigators know from the start that they won't be able to monitor a suspect's phone or social media, for example because the suspect is an anarchist known to have good security, and from the start they resort to physical surveillance.

And the thing is, all of this applies both to Europe and to the U.S. So, why does physical surveillance feel more common in Europe than in the U.S. in recent years? I believe it is simply because in recent years, anarchist attacks viewed by the State as more threatening, such as arson attacks, have been more common in Europe, which has led to a higher number of severe repressive operations, and severe repressive operations are more likely to feature physical surveillance. Roughly, I'd say that there has been a drop in "high-profile" anarchist attacks in the U.S. between the end of the Green Scare in the 2000s and the 2020 uprising. This has led to fewer severe repressive operations, and thus to fewer cases of physical surveillance. Interestingly, our Threat Library references two repressive operations from the U.S. that involved physical surveillance, one is from 2000 and one from 2023, but of course this could be a sampling bias.

So, in short: physical surveillance is probably used in the U.S. too, in particular in places where arson attacks have recently been claimed by anarchists. U.S. anarchists could anticipate the use of physical surveillance by developing an appropriate skill set. To help with that, we've recently translated to English a comprehensive German zine on the topic called "Measures Against Surveillance", which can be found on our website.

A second issue you mention is the impact of E.U. privacy laws on police investigations. I believe this impact is minimal; E.U. privacy laws mostly apply to private companies and not to law enforcement. Police in Europe can and do routinely request data from social medias, email providers, Internet Service Providers, and so on.

But then, the question remains: what are the differences in State repressive techniques between countries, and how can we take these differences into account? This is a good question, and I don't have a comprehensive answer for it, but I can try to discuss a few examples. As you said, doorbell cameras such as Amazon Ring are particularly widespread in the U.S., which increases the need to dress anonymously when traversing residential neighborhoods during an action. Compared to Western Europe, I think the U.S. justice system more frequently offers immunity or reduced sentences in exchange for snitching, which should probably be taken into account, but how, I don't know. The practice of hiding microphones and cameras in apartments and GPS trackers on cars seems more widespread in Italy. The use of torture in police custody is more routine in Belarus and Russia. I suspect that the United Kingdom employs more long-term infiltrators than other European countries, but this is hard to quantify.

TFSR: You make good points.

Considering the tools and technology widely available, the question of where do the devices displayed at notrace.how come from bubbles up in my mind. Have comrades been able to determine the sources of the surveillance tools used against them, if they're coming from personal / social enemies, bosses or mafia, political enemies like authoritarians or fascists, or state actors?

Aster: Ah, yes, you're talking about our Ears and Eyes project, that lists cases of hidden surveillance devices such as microphones and cameras in apartments, or GPS trackers on cars. We currently list more than a hundred devices, with vast disparities between countries, for example we have 50 cases from Italy but only 5 from the U.S. To answer your question, in most cases, no, comrades are not able to conclusively determine who installed a device. This is because most of the time, when a device is discovered, the spies don't try to retrieve it, or even acknowledge it, and of course their name isn't written on it.

This being said, I believe that the vast majority of the devices we list have been installed by State actors. To determine this, we can use two clues. The first clue is the context. If a device is found by people who are likely to be under investigation and don't have many personal or social enemies, the device was probably installed by law enforcement. The second clue is the device itself: its components, and how it is assembled. Non-State actors tend to use store-bought devices. State actors tend to use either devices supplied by specialized companies that often only market them to law enforcement, or devices that they manually assemble themselves.

TFSR: Similar to the question of sources of the technology, because the tools, tech and knowledge is more ubiquitous it would seem that notraces. how offers a lot of opportunities for counter-surveillance through reverse engineering those devices. Can you speak about this?

Aster: Well, on our side, generally all we have access to is a brief description of a device components, and sometimes pictures, which is not enough for reverse-engineering. This is because we only document what people publish online. But for the comrades who discover a surveillance device, I agree that there's a good opportunity for reverse-engineering, and I would encourage comrades who find a device to try to disassemble it, understand it, and publish their findings online, if they can do so safely. For example, if a device has an SD card, analyzing its contents, including by attempting to restore deleted files, could give clues to when the device was installed and how it operated. If a device has a SIM card, analyzing its contents with a SIM card reader could give clues to the identity of the spies. Recently, the SD card of a bug found in an anarchist library in France was analyzed, which revealed a few details about the device.

TFSR: Yeah, that example is really interesting. Listeners can find information on this by searching for the Libertad anarchist library in Paris. I saw a post about it on anarchistnews.org some time ago that pulled from Ears and Eyes.
It strikes me that people have to be paying a lot of attention to their surroundings when they'll notice that there's a small camera pointed at them from the skylight of a nearby building or the back window of a van parked for too long on their street. This says nothing of finding a microphone installed inside of their photocopy machine leaching tiny bits of electricity such as in the case of the Libertad library in Paris. How do people find these and what does it mean to have an intimate knowledge of your surroundings to pick out what is out of place? Are there techniques or tools that are suggested for this sort of exploration?

Aster: About how people find these devices, sometimes it's just by chance, for example in the case of the Libertad library in Paris, the comrades were simply dismantling the photocopy machine for repairs when they found the bug. And sometimes, people specifically search for surveillance devices and find some.

In my opinion, if you suspect that a place or vehicle might be bugged and you want to search for surveillance devices, the first thing you should do is a manual, visual search. For this, you need to know where devices are typically hidden, our website can help with that.

- In the case of a building, devices are often hidden next to a power source, so they can be connected to it instead of needing a battery. You can take a screwdriver and other tools and dismantle power outlets, multi-socket adapters, ceiling lights, any electrical appliances, and look for anything that shouldn't be there. You can also look inside furniture, basically anywhere a device could fit. This is a long process, it can take several hours for a single room.
- In the case of a vehicle, devices are either hidden outside the vehicle, typically under it, or inside the vehicle. You can start by taking a look under the vehicle, inside wheels, on rear bumpers, behind ventilation grids, looking for anything that shouldn't be there. Then you can take appropriate tools and dismantle the interior, the ceiling, the dashboard, the seat heads, and so on. Devices can also be hidden in motorbikes or bicycles, for example inside or under the seats.
- In the case of a camera installed at a window of a nearby building, you might be able to detect it binoculars, but of course it's a bit tricky.
- In the case of a camera installed in a surveillance vehicle in the street, this is where

having an intimate knowledge of your surroundings, as you said, can be useful. I'll briefly explain a specific technique to detect a surveillance vehicle with a camera pointed at your home. This technique only works if you live in a place where there aren't too many different vehicles that park, so it works in some residential areas in cities and in most rural areas. Basically, each time you exit or enter your home you take note of all the vehicles parked in the street that have a line of sight to your home. You take note of their model, color, and license plate, you remember the information or you write it down, as you prefer, but if possible you try to do this without looking suspicious. After some time doing that, you will be familiar with the "baseline" of vehicles that park in your street, which will be the vehicles of people who live nearby or their guests. Once you're familiar with the baseline, you can spot vehicles that are not part of this baseline and scrutinize them carefully to check if they are surveillance vehicles.

Specialized detection devices also exist, for example radio frequency detectors to detect devices transmitting data on radio frequencies, or camera lens detectors. I don't have experience with these detection devices so I don't feel confident to talk about them, but I think they can be a valuable option that should be researched.

Also, one thing that should be remembered is that, when searching for bugs, you cannot rule out false negatives. If you don't find a bug, maybe there is one that you missed. And even if you do find a bug, maybe there are others that you missed. I think the point of searching for bugs should be to prevent the State from gathering information about us, and not to consider a space to be free from surveillance devices. For example, I think that sensitive, incriminating conversations should not take place even in buildings that have been searched for bugs, and should always take place outdoors and without electronic devices.

One last thing I want to note is that another option to counter this threat is to try to prevent the installation of surveillance devices in the first place. To install a device in a building or vehicle, the State needs to access this building or vehicle. In the case of buildings, they typically make a covert entry when the occupants are not there, either by picking the lock or asking the building owner for the keys: this can be countered by making sure there's always someone in the building, or by installing our own video surveillance system to monitor the building when we're not there. In the case of vehicles, they typically install devices on vehicles parked on public streets: this could be countered by never parking on public streets, but of course this isn't always possible.

TFSR: In closing, I've seen activists over the years talking about engaging in conflict and the repercussions they could experience from it in individual terms, ignoring the social impact of state crackdowns and the network ef-

fect of counter-insurgency. Would you mind saying a bit about counter-surveillance and security culture as community defense?

Aster: For sure, repression can disrupt networks, in both material dimensions, for example by sending people to jail, and psychological dimensions, for example by spreading fear and distrust. We've already talked about the material dimensions in the rest of this discussion. I can talk about two things that I think we can do to address the psychological dimensions.

The first thing is to find the right balance in how we mentally approach State repression. Specifically, I think we should avoid thinking both that we are *powerless in face of repression* and thinking that *repression will never strike*. We are not powerless because we can organize, we can take measures against surveillance, we can avoid repression, we have agency. But it's equally wrong to think that repression will never strike, because we can't be sure of that, even if we take a lot of precautions there's always chance and things we can't predict. I think that if we manage to find this balance, then if a comrade gets caught or if we get caught ourselves we will know that we did our best to prevent that from happening, but we also won't be taken by surprise.

The second thing is that we *can* prepare for repression. We can discuss with our friends about our fears of getting caught. We can make sure that the people who get arrested have lawyers. We can support our prisoners and make sure we include them in our struggles. If we prepare for repression, we'll be less taken by surprise if it strikes.

TFSR: Aster, thanks so much for the time you took for this conversation and for the work that y'all are doing. Solidarity and appreciation to you!

Aster: Thanks for the interview! It was a good opportunity for me to reflect on our work, it was really helpful.

THE Final Straw

A WEEKLY ANARCHIST SHOW

The Final Straw is a weekly anarchist and anti-authoritarian radio show bringing you voices and ideas from struggle around the world.

You can send us letters at:
The Final Straw Radio
PO Box 6004
Asheville, NC 28816
USA

Email us at:
thefinalstrawradio@riseup.net
or **thefinalstrawradio@protonmail.com**

To hear our past shows for free, visit:
https://thefinalstrawradio.noblogs.org

To support transcription and zine-making efforts which are funded by donations, visit:
https://thefinalstrawradio.noblogs.org/donate/
or via Patreon:
https://www.patreon.com/tfsr
or via LiberaPay, which does not take a cut of the payments:
https://liberapay.com/The-Final-Straw-Radio/